NPS-CS-08-008

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

A FIELD STUDY OF AN IRIS IDENTIFICATION SYSTEM

by

Simon McLaren
Simson L. Garfinkel

1 May 2008

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

NAVAL POSTGRADUATE SCHOOL
Monterey, California 93943-5000

Daniel T. Oliver
President

Leonard A. Ferrari
Provost

Reproduction of all or part of this report is authorized.

This report was prepared by:

Simon McLaren
Student

Simson L. Garfinkel
Associate Professor

Reviewed by:

Peter Denning
Department of Computer Science

Released by:

Dan C. Boger
Interim Associate Provost and
Dean of Research

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

1. REPORT DATE *(DD–MM–YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From — To)*
27–3–2009	Technical Report	2008-01-01—2008-07-31

4. TITLE AND SUBTITLE

A field study of an iris identification system

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Simon McLaren, Simson L. Garfinkel

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Naval Postgraduate School
Monterey, CA 93943

8. PERFORMING ORGANIZATION REPORT NUMBER

NPS-CS-08-008

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

We conducted a field trial of a commercial iris identification scanner at the US Navy Fleet Numerical Meterology and Oceanography Center (FNMOC) in Monterey, CA. Scans were performed by US military guards who had received approximately 20 minutes of training in the use of the scanner. Operating the iris scanner in a one-to-many subject identification mode, we experienced no false acceptances and few false rejects. But we did find the PIER 2.3 scanner to be highly sensitive to the position of the sun with respect to the scanner and subject.

15. SUBJECT TERMS

Iris Scanning; SecuriMetrics; L-1; PIER 2.3

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(include area code)*
Unclassified	Unclassified	Unclassified	UU	17	

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

We conducted a field trial of a commercial iris identification scanner at the US Navy Fleet Numerical Meterology and Oceanography Center (FNMOC) in Monterey, CA. Scans were performed by US military guards who had received approximately 20 minutes of training in the use of the scanner. Operating the iris scanner in a one-to-many subject identification mode, we experienced no false acceptances and few false rejects. But we did find the PIER 2.3 scanner to be highly sensitive to the position of the sun with respect to the scanner and subject.

1 Introduction

Iris scanning is rapidly emerging as a biometric of choice for both identification and identity verification. Compared with other biometrics in use today, iris scan biometrics have the advantage of being *contactless* (eliminating the dirt and hygiene problems associated with finger scanning); *fast*; and *highly individualistic* (with an estimated 173 bits of entropy in each iris template[4]). What's more, iris scanning does not require special acquisition hardware: identification using iris scan technology has been performed using ordinary photographs acquired with commercial 35mm film. Indeed, several companies are developing iris scanners which can covertly acquire iris scans—potentially even through the glass of a car moving at highway speeds. Some companies are currently researching the use of a cell phone camera as a capture device.

1.1 Motivation

Iris scanning is being increasingly deployed by civil air authorities at airports for passenger identification[7] and in military efforts to distinguish between friendly and insurgent elements of civilian populations. According to L-1 Identity Solutions, a leading vendor of iris identification systems, there are more than 2,000 PIER (Portable Iris Enrollment and Recognition) devices deployed today "throughout Iraq, Afghanistan, Pakistan, Cuba, Bosnia and other areas of conflict."[11]

This experiment was intended to test the reliability of a handheld iris scanner in outdoor field conditions. This test is necessary because, while iris scanning is used being used around the world, all reports that we have read discuss its use in office-like environments where the environmental conditions are fairly stable and there is an expectation of cleanliness. A search of the literature found little data on the reliability of iris scanners in less-than-ideal conditions. For example, although iris scanners are widely used in Iraq by US forces, the only published photographs that we can find show the scanners being used inside tents—locations where the glare of the sun, fog and driving rain are not a factor.

We envision a future in which iris scanning might be used under less-than-ideal conditions, for example, at a maritime port or at a highway check point. Compared with other biometrics such

Figure 1: The L-1 Identity Solutions/SecuriMetrics PIER 2.3. This handheld device weighs 16 oz. and stores up to 400,000 templates in onboard memory for local matching. The back side of the PIER (right) shows the camera and the infrared illuminator.

as fingerprints or facial recognition, iris scanning would seem to have an advantage in these environments: even when a person's hands are covered with gloves and the face is bundled up, the eyes (and the irises) are still visible.

Before we can recommend that iris scanning be considered for these environments, we felt that it was necessary to actually test an iris scanner in a realistic field environment and see how it performed.

1.2 This Paper's Contribution

This paper presents the results of a qualitative pilot study in which volunteers were used to both operate an iris scanner and as the scanner subjects. In our review of the academic literature we found many articles discussing privacy and other social implications of biometrics, but we did not find a single field study exploring the actual use of the technology.

2 Experimental Set Up

2.1 Location

The experiment was conducted at the Fleet Numerical Meteorology and Oceanography Center (FNMOC) located in Monterey California, approximately 1 mile from the shore line of Monterey Bay. This location appeared ideal as it would likely provide weather conditions similar to those present at the gate of a typical port facility. As FNMOC is a gated facility, the iris scanner could be used on volunteers as they entered the facility and while they where still inside of their vehicle.

2.2 Iris Recognition Hardware

We used a PIER 2.3 (Portable Iris Enrollment and Recognition) manufactured by SecuriMetrics (which was acquired by L-1 Identity Solutions in 2006). This is the same iris scanner that is used by US forces in Iraq. The PIER 2.3 implements the iris identification algorithm developed by John Daugman[3]. This device is also the top-performing "Product A" which the IRIS06 Iris Recognition Study determined to have the best recognition accuracy of the units tested.[1, 12] Perhaps most importantly, the PIER 2.3 was the only handheld iris that we could find available in the US market.

The PIER 2.3 is a ruggedized battery-powered handheld iris scanning unit that is capable of performing both registration of iris templates and recognition of irises in the field. The unit can be operated as a stand-alone unit or in a tethered mode with an external control. It can hold 400,000 iris templates in its on-board computer, and weighs roughly one pound.

The PIER's front side has a small screen and keyboard. The back side has an infrared illuminator and a fixed-focus camera.

The PIER software has two primary modes of operation. In *registration mode*, new subject eyes are scanned and stored in the computer's database. Each eye may be annotated with a name and additional information. In *identification mode*, the PIER compares an eye being scanned with its internal database and reports if there is a match.

Because the camera is fixed-focus, it is the responsibility of the operator to hold the camera at precisely the correct distance from the person being scanned. Focusing is assisted by two indicators on either side of the PIER's display. Focusing is rated on a scale of 0–100%. A bar on the left-hand side of the screen indicates the degree of focus from 0–90%, while a bar on the right-hand side indicates focus from 90%–100%. (The PIER software requires that an iris image be focused to at least 90% in order to register a subject.) In practice, the operator holds the camera between 4" and 6" from the subject's eye and slowly moves the camera back and forth until the left hand bar extends from the bottom to the top of the display and the right hand bar is as high as possible (see Figures 2 and 3). Although this procedure sounds awkward, in practice it is quite easy to use.

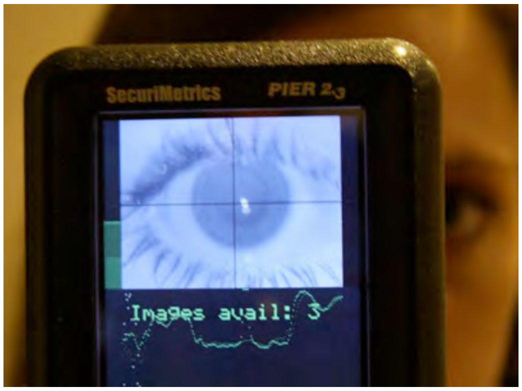

Figure 2: An iris being scanned, note the green bar to the left of the image. The left bar graph indicates the amount of focus from 0–90%, with 90% being indicated by a green bar that extends from the bottom of the display to the top. A bargraph on the right hand side of the image (shown in Figure 3) indicates focus from 90%–100%.

Figure 3: This image shows an acceptable iris image as indicated by the full green bar to the left of the iris image and partial green bar to its right. These green bars indicate the quality of the image being captured. It is desirable to collect images where at least a portion of the right green indicator is visible.

Gender	N
Male	21
Female	4
Total	25

Table 1: Gender of the scanner subjects.

2.3 Subjects

Subjects were recruited with an e-mail solicitation. All subjects were either members of the U.S. Navy, DoD civilian Employees or DoD civilian contractors and worked at FNMOC. A total of 25 subjects both responded to the e-mail and agreed to take part in the experiment. Demographic information appears in tables 1 through 4.

Each subject was assigned a subject number and given a window placard with a green dot that displayed their subject number.

Four of the subjects who responded to the e-mail were trained US Military guards who provide border security for FNMOC. These subjects are experienced at standing watch and screening vehicles. They were given the additional role of *scanner operators* and were trained to use the PIER 2.3 by Simon McLaren, who in turn was trained to use the scanner by SecureiMetric. The operators were also shown a training DVD provided by SecuriMetrics.

2.4 Registration and Scanning

We registered the volunteers during the first week of the experiment. Subjects were registered in a typical office-like environment with moderate ambient light. Both the left and right eyes

Color	N
Blue	10
Blue-Green	1
Brown	7
Dark Brown	1
Hazel	6
Total	25

Table 2: Eye color of the 25 scanner subjects.

Age	N	
20–29	8	(32%)
30–39	4	(16%)
40–49	6	(24%)
50–59	6	(24%)
60–	1	(4%)
Total	25	

Table 3: Age of the 25 scanner subjects

were registered; although the PIER 2.3 has the ability to record a subject name, we only stored the subject's number in the handheld unit.

2.5 The Spoiler

One volunteer was chosen at random not to be registered in the PIER 2.3. The subject nevertheless was given a sticker for their vehicle just like all the other volunteers. This volunteer agreed to have their iris scanned each day during the experiment to allow for an opportunity for a false accept within the limits of our small sample set. This was to simulate a scenario where someone who was not authorized to access the port was seeking access: We wanted to see if the PIER 2.3 would correctly fail to recognize this individual.

Corrective Lenses	N	
None	12	(48%)
Soft Contacts	3	(12%)
Hard Contacts	1	(1%)
Glasses	7	(28%)
Both Contacts and Glasses	2	(8%)
Total	25	

Table 4: Corrective Lenses used by the 25 scanner subjects.

2.6 Test Scanning

We conducted the scanning trial during the second week of the experiment. Scanning subjects were instructed to drive onto the facility and, after receiving official permission to enter, the subject would stop their vehicle near the scanner operator. The scanner operator would then greet the subject and ask if it was okay to scan their iris. If permission was given the operator would proceed to position the scanner the recommended 4" to 6" from the subject's eye and attempt to collect a scan of their iris.

- If the scan was successful the operator checked to see if the subject number displayed by the scanner matched the subject ID number on the subject's placard. The operator also recorded whether the subject was wearing glasses or contacts and estimated the amount of time that it took to scan and identify the subject.

- If the scanner failed to recognize the subject, the operator would record the same information and complete a short form recording any observations they noted that might have contributed to the failure to recognize. The operator would then try the scan again, and again would record the same information. The operators where told not to attempt to recognize a subject any more than three times on a single attempt to enter the facility.

If a subject entered on foot, the procedure was the same, with the exception of the subject standing still in front of the operator instead of sitting inside a car. The operator recorded the same information about the attempt and success or failure.

Scans were performed from 0730–0930 and from 1130-1130 on each day of the experiment, these times being chosen to match the morning commute and lunch hours of FNMOC. This allowed for the possibility of scanning each subject at least twice each day, and increased the likelihood of being able to scan those subjects that usually arrived prior to 0730 in the morning on their return from lunch.

2.7 Eyeglasses

SecuriMetrics specifically recommends against enrolling through eyeglasses. But given our scenario that the iris scanner would eventually be used at a gated facility by people entering the facility in vehicles, it seemed reasonable to assume that some drivers would be wearing eye glasses and would forget to remove them on occasion, even if they were trained to do so.

Therefore, subjects who wore eyeglasses glasses were instructed to remove them or lift them over the eyebrows to be scanned on Monday and Tuesday. Wednesday through Friday subjects who wore glasses were instructed to leave them on as the experiment attempted to determine how eye glasses affected the reliability of the device.

3 Results

We successfully registered all 25 scan subjects during the first week. During the second week the guards performed scans at 100 gate crossing events, of which 93 were for registered volunteers and 7 were the spoiler.

3.1 Difficulty in Registration

Two of our 25 subjects had a difficult time registering. Both required multiple attempts to acquire acceptable images of at least one eye during registration. We don't know why these two subjects had difficulty registering, but because the initial registration was indoors, weather would not be a factor. It may be that the two subjects moved around too much. Or it may be that there was something about their eyes which confused the PIER 2.3 software.

3.2 Time to scan

Time-to-scan reported by the operators ranged from four to 15 seconds, with a reported average of six seconds per scan. An additional three to five seconds was then required for the scanner operator to visually verify the identity by examining the vehicle placard.

Drivers were also required to come to a complete stop for the scanning to take place. This added an additional 10 to 20 seconds to the entry time at the gate. However, drivers are presently required to stop and undergo an ID check with the guard manning the gate. If the scanning had been conducted by this guard, rather than by a operator at a second location, the added time due to the stop would have been negligible.

3.3 False Acceptance

We did not experience a single false acceptance or misidentification during our experiment. All successful scans correctly identified the subject in question. The unit never mis-identified the "spoiler."

3.4 False Rejection

The system recorded six false rejections out of 93 attempts for the registered users, for an overall false rejection rate of 6.4%. Figure 4 shows the fraction of identification attempts requiring a second and third scan.

3.5 "Sheep" and "Goats"

Out of 24 registered subjects, 13 (54%) never received a false rejection, while 11 (46%) experienced at least one false rejection on a first attempt. Four of our subjects (17%) experienced false rejections on 50% or more of their first attempts. While some of these failures might be explained by the environment, at least one subject commented that she "seemed to always get rejected" by the device.

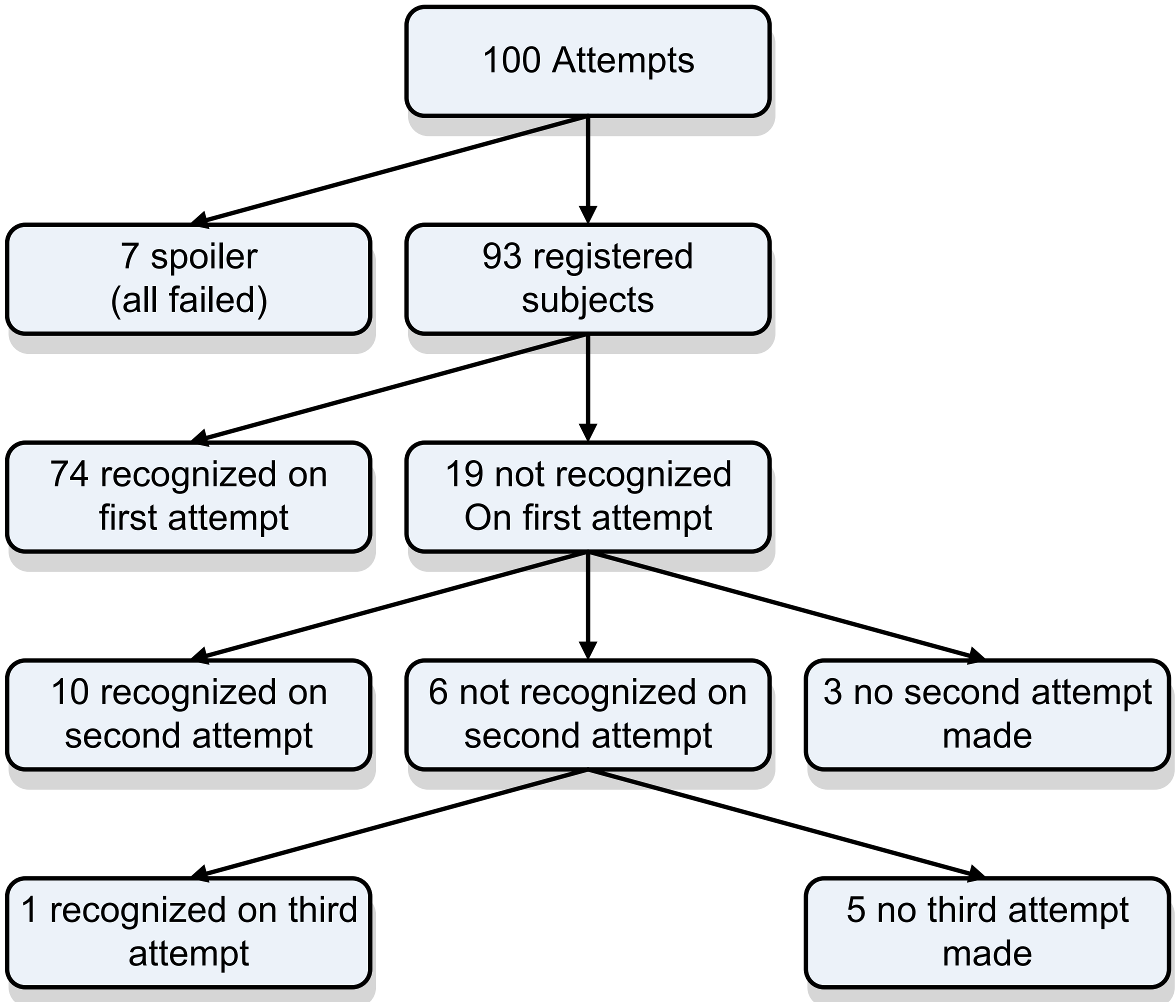

Figure 4: Breakdown of the 100 scan attempts showing cases where second and third scans were necessary.

Doddington *et al.* observed the tendency of biometric speech recognition systems to favor some users and disfavor others; they introduced the term *sheep* for individuals who were easy to identify and *goats* for those who are hard to identify[5]. We believe that we were seeing similar results in our limited study size.

3.6 Factors leading to poor scans

We discovered several factors leading to poor scans: eyeglasses, poor lighting, and motion.

3.6.1 Eyeglasses

Only six gate crossing events involving eyeglasses were recorded when subjects wore glasses. Of these six attempts, three were successful. Of the three that failed, one was successful when the glasses were removed, one was unsuccessful when the glasses where removed, and one subject did not consent to a rescan without glasses.

3.6.2 Lighting

Recognition failures were reported by the guards when there was sunlight either behind or in front of the subject:

- One of the volunteers experienced a false rejection on the first attempt when they walked up to the operator. The operator noted that the sun was directly behind the subject. Once again, this is a condition in which the manufacturer specifically states the PIER 2.3 should not be used: A bright light behind the subject creates an image that is back-lit and can significantly reduce the quality of the image captured by the iris scanner. The operator reported changing the relative position of the subject with respect to the sun and the second attempt resulted in a correct match.
- A second, unanticipated scenario involved the sun being low on the horizon and directly behind the operator. This placed a good deal of bright light directly into the face of the subject and resulted in at least three false rejections. The Day 1 operator quickly adapted to this situation by placing his body between the sun and the subjects, thereby casting his shadow on the face of the subject on subsequent scans. The adaptation eliminated the bright light in the faces of the subjects, and improved the success rate of the scanner. The Day 1 operator passed along his experience and solution to the rest of the operators, who then incorporated the solution when they operated the scanner.

We can think of three potential causes for bright light in the face of the subject causing increased false rejections:

1. Too little iris visible: The bright light might have aused the subjects to squint. This would have resulted in a much greater portion of the iris being occluded, without enough iris visible to the scanner to get a match.
2. Too much iris visible: The bright light in the subject's face would likely cause the pupil of the iris to contract to a greater extent than when the subject was registered in an office-like light setting. This would have resulted in more iris being exposed, which might be inconsistent with the amount of iris visible at the time of registration.
3. Glare: The bright light in the subject's face might have produced a significant glare on the reflective surface of the iris. This would have resulted in an occlusion of a portion of the iris in the image that was captured by the scanner.

Regardless of the physical connection between the sunlight shining in the face of the subject, its effective pupil size, eyelids or surface reflection of the eye, or the impact on the image collected by the iris scanner, the solution was to block the source of light. In an office environment the light source may be positioned so it will not cause interference. But the sun will present issues with the current generation of iris recognition hardware and algorithms if the iris scanner is mounted in a fixed, outdoor position.

3.7 Motion

The PIER 2.3 has a frame rate of 15 fps. Given this low rate, it seems reasonable to conclude that some of the difficulty in obtaining clear photographs is not due to focusing but a result of motion blur. Motion blur is likely to be more of an issue outdoors where human movement can be induced by the wind or cold temperatures. Using a camera with optical image stabilization and a deeper field of view would help resolve this problem.

4 Subject Concerns

In our attempts to recruit subjects for the study we encountered two concerns which prevented people from participating in the study.

The first concern was that the iris scanner might cause some kind of physical injury. Although some subjects were set at ease when they were told that the "scanner" was really nothing more than a camera with a infra-red light similar to a video camera with a night vision feature, others remained hesitant. We believe that calling the process something other than "iris scanning"—perhaps calling it "iris recognition" or even just "eye photography"—might reduce some fears.

Other individuals expressed concern with providing their iris template to a government official. Despite assurances that the iris template collected for the experiment would at no point be associated with their name and would be destroyed at the end of the experiment, some individuals where still quite hesitant about giving up such a highly identifying "image." This concern was somewhat surprising, given that this "mistrust" came from individuals who were actively employed by the US Department of Defense. This highlights the need to provide individuals who may be forced to utilize such devices with assurance of how their biometrics will be used.

A person may have increased level of trust of government if the person is made aware of the penalty to government or governement officials that would result if information collected is misused or used for a purpose other than that for which it was originally intended. What incentive does the government (or any enterpise for that matter) have to play by the rules? While government, with the help of it legislative arms, can change those rules, at least those changes can be debated in an open forumn prior to being allowed by enactment of law.

5 Lessons Learned

We encountered many short comings in our experimental protocol during the field study. Although we did not have the time to rectify these problems, we present our lessons learned with

the hope that others may benefit from our experience.

1. We intentionally trained the scanner operators and then allowed them to scan the subjects without monitoring to produce realistic field conditions. In retrospect, it would have been useful to quietly observe the guards using the PIER 2.3.

2. It would have been useful to survey the experimental subjects before and after the study to see how their views of biometrics were affected by experiencing the process. We chose not to do this because we wished to minimize the impact of the study on our volunteers.

3. It would have been useful to test the PIER 2.3 under low-light or nighttime conditions. Both of these light conditions are likely in any outdoor deployment of iris scanners used to confirm the identity of an individual seeking access to a gated facility.

We believe that the FRR rate would be significantly improved through better training and monitoring of the operations. Many factors, including the angle of the device to the subject, have a critical effect on the performance. Most rigorous biometrics studies show iris FRR in the 0.X to 2.X range (worst case) considering the varied protocols. Therefore the numbers are quite high and may be viewed as anomalous in the community.

6 Future Work

As indicated, there has been remarkably little work evaluating the effectiveness of iris recognition systems under real-world conditions. Clearly, it would be useful to repeat this experiment with a larger user population, more verification attempts, and a longer time period.

Future work should perform more detailed data collection to determine if the same individuals are consistently having problems being scanned, or if these problems are correlated with the scanner operator, the time of day, weather, or lighting conditions.

Because individuals are likely to use eye glasses, more work needs to be done to determine the impact that glasses wearing has on the accuracy of the scanner.

It would also be useful to evaluate iris recognition systems under a variety of other real-world conditions. For example, how do these systems behave in windy environments or during storms?

Finally, it would be useful to test an iris scanner with a prosthetic human eye or a contact lens to determine if the system is susceptible to the same kinds of attacks as fingerprint scanners[9].

7 Related Work

Coventry *et al* discussed issues regarding self-service biometric verification and usability, but did not perform a field study[2].

Matey *et al.* developed an iris identification system that could capture iris scans of walking individuals and identify them using the Daugman algorithm. They used a PIER 2.3 camera from SecuriMetrics to enroll 119 volunteer Sarnoff employees, and then performed multiple tests of each employee walking through their prototype "Iris on the Move" system[8].

Fancourt *et al.* have demonstrated iris recognition systems that can capture images at two meters from non-cooperating individuals[6].

Newton *et al.* conducted a meta-analysis of third-party evaluations of iris recognition systems and found that "despite differences in methods, hardware, and/or software, all three studies report error rates of the same order of magnitude: observed false non-match rates (FNMRs) from 0.0122 to 0.3847 at a false match rate (FMR) of 0.001."[10]

IRIS06 noted that "eyeglasses can degrade iris recognition performance" and tested Products A, B and C both with and without "test subjects wearing eyeglasses." The report found that "Product A matching performance is similar both with and without glasses."[1] In a separate publication, one of the report's authors identified "Product A" as being the PIER 2.3[12].

8 Acknowledgments

Funding for this project was provided by the Naval Postgraduate School's Research Initiation Program.

The PIER 2.3 unit was provided on loan by SecuriMetrics, which asked to review a copy of this paper as a condition of the loan.

References

[1] Authenti-Corp. Iris recognition study 2006 (iris06): Aka standards-based performance and user cooperation studies of commercial iris recognition products, Sept. 1 2007.

[2] L. Coventry, A. D. Angeli, and G. Johnson. Honest its me! self service verification. In *Workshop on Human-Computer Interaction and Security Systems*, Apr. 5–10 2008.

[3] J. Daugman. How iris recognition works. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1):21–30, 2004.

[4] G. I. Davida, Y. Frankel, and B. J. Matt. On enabling secure applications through off-line biometric identification. In *Security and Privacy 1998 Proceedings*. IEEE, May 3–6 1998.

[5] G. Doddington, W. Liggett, A. Martin, M. Przybocki, and D. Reynolds. Sheep, goats, lambs and wolves a statistical analysis of speaker performance in the nist 1998 speaker recognition evaluation. In *The Proceedings of The 5th International Conference on Spoken Language Processing*, Nov. 30 – Dec. 4 1998.

[6] C. L. Fancourt, L. Bogoni, K. J. Hanna, Y. Guo, R. P. Wildes, N. Takahashi, and U. Jain. Iris recognition at a distance. In *AVBPA*, volume 3546 of *Lecture Notes in Computer Science*, pages 1–13. Springer, 2005.

[7] T. Jowitt. Uk airport gets iris recognition program. *ComputerWorld Security*, Jan. 24 2008.

[8] J. Matey, O. Naroditsky, K. Hanna, R. Kolczynski, D. LoIacono, S. Mangru, M. Tinker, T. Zappia, and W. Zhao. Iris on the move: Acquisition of images for iris recognition in less constrained environments. *Proceedings of the IEEE*, 94(11):1936–1947, Nov. 2006.

[9] T. Matsumoto. Gummy and conductive silicone rubber fingers: Importance of vulnerability analysis. In *AsiaCrypt 2002*, Dec. 1–5 2002.

[10] E. M. Newton and P. J. Phillips. Meta-analysis of third-party evaluations of iris recognition. Technical Report 7440, National Institute of Standards and Technology, Aug. 2007.

[11] V. Technology. Viisage to acquire leading iris recognition company securimetrics, creating the industry's only u.s.-based finger, face and iris multi-modal biometric offering, Feb. 6 2006.

[12] V. S. Valencia. Current state of iris recognition performance: Image quality and interoperability. In *Panel on Advanced Technologies for Iris Recognition, Biometrics Consortium Conference*, Sept. 12 2007.